Installing the Operating System on the Cisco Unified Communications Server, Versions 2000.4.3 and 2000.4.3a

Note This document supports operating system installations 2000.4.3 and 2000.4.3a; it also supports operating system upgrade 2000.4.3a.

Use this document as a guide for installing the Cisco-provided Windows 2000 operating system on the Cisco Unified Communications server. Cisco Unified Communications applications that use this operating system include Cisco Unified CallManager, Cisco Personal Assistant, Cisco Emergency Responder, Cisco Unified Contact Center Express, Cisco Unified IP-IVR, Cisco Unified IP Queue Manager, Cisco Conference Connection, Cisco Unified Customer Voice Portal, and Cisco Unified MeetingPlace Express.

Purpose of Document

This document includes information and procedures for the following topics:

- Installing the operating system
- Applying software updates; for example, hotfixes, BIOS updates, service packs, and operating system upgrades

Use this document with the documents that are listed in the "Related Documentation and Software" section on page 4.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Revision History

Table 1 provides the revision history of this document.

Table 1 Revision History of This Document

Revision Date	Comment
July 5, 2006	• Updated the "Important Considerations" section on page 6. • Updated the list of applications that are supported; see the "Which Cisco Unified Communications applications use the Cisco Unified Communications operating system?" section on page 8. • Included information about the operating system 2000.4.3a upgrade; see the "Frequently Asked Questions About Operating System Software Updates" section on page 24 and the "Installing Operating System Software Updates" section on page 26. • Updated the "Error Messages" section on page 28. • Removed specific information from the "Hardware Requirements" section on page 6; included the specific information in the operating system release notes.

Contents

This document includes the following topics:

- Revision History, page 2
- Conventions, page 4
- Related Documentation and Software, page 4
- What's Changed in This Release, page 5
- Hardware Requirements, page 6
- Important Considerations, page 6
- Frequently Asked Questions About the Operating System Installation, page 7
  - What hardware and disks do I receive when I purchase a Cisco MCS or a Cisco Unified Communications application?, page 7
  - Can I install this version of the Cisco Unified Communications Server operating system on any Cisco MCS?, page 8
  - How long does it take to perform the operating system installation?, page 8
  - Which Cisco Unified Communications applications use the Cisco Unified Communications operating system?, page 8
  - How does the operating system installation work?, page 9
  - What data must I provide to configure the server?, page 9
  - Which Cisco-verified, third-party applications may I install on the server?, page 13

  - Which Cisco Unified Communications applications may I install on the same server as Cisco Unified CallManager?, page 14
  - May I run a web browser on the server?, page 14
  - What preinstallation tasks should I perform?, page 16
  - How do I connect the keyboard and mouse to the server?, page 16
  - What if I encounter problems during the installation?, page 16
  - Where do I obtain the release notes?, page 17
- Installing the Operating System, page 17
- Performing Post-Installation Tasks, page 19
  - Configuring Network Settings, page 20
  - Verifying the Operating System Version, page 22
  - Uninstalling Microsoft Hotfix 831877, page 22
  - Applying Additional Security, page 23
- Frequently Asked Questions About Operating System Software Updates, page 24
  - Why can I not find the web executable that the Cisco Unified Communications application documentation specifies?, page 24
  - In what order should I apply the software updates?, page 24
  - How long does it take to upgrade the operating system?, page 24
  - Where do I find more information (release notes/readme) about the software update?, page 24
  - When should I install the software update?, page 24
  - Which versions of the operating system are compatible with operating system upgrade 2000.4.3a?, page 25
  - May I perform configuration tasks during the update?, page 25
  - May I use Terminal Services, VNC, or ILO on this server during an update?, page 25
  - What pre-/post-update tasks should I perform?, page 26
  - What if I encounter problems during the operating system upgrade?, page 26
- Ongoing Server Management, page 28
- Error Messages, page 28
- Using the Bug Toolkit, page 33
- Obtaining Documentation, page 33
- Documentation Feedback, page 34
- Obtaining Technical Assistance, page 35
- Obtaining Additional Publications and Information, page 37

Conventions

The following documentation conventions apply to this document:

Blue Text—To quickly navigate to a section or URL, click text that appears in this color.

Note Reader, take note. Notes contain helpful suggestions or references to material that is not covered in the publication.

Tip Reader, use the information to perform a task. Tips provide helpful information for performing tasks.

Caution Reader, be careful. You may do something that could result in equipment damage or loss of data.

Unless otherwise indicated in this document, Cisco Unified CallManager refers to supported versions of Cisco CallManager and Cisco Unified CallManager.

Related Documentation and Software

Review the following documents before you install the operating system:

- The readme document that posts on the web next to the operating system upgrade, if available

  This document provides a list of changes from the last release and additional information about the operating system.
- *Cisco IP Telephony Operating System, SQL Server, and Security Updates*

  This document provides information for tracking Cisco-supported operating system, SQL Server, and security files that are available for web download from the web.
- The appropriate Cisco Unified Communications application documentation

  Locate the release notes, installation/upgrade/backup and restore documents, and configuration guides for the applications that you want to install or upgrade.

As you review this operating system document and perform operating system installation and upgrade procedures, use Table 2, which provides URLs for software and documentation.

Table 2 Quick Reference for Documentation and Software URLs

Related Information and Software	URL
Server hardware specifications	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html (for Cisco MCS) http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html (for Cisco-approved, customer-provided servers)
Related operating system and server documentation, which includes the following documents: • Installation document and release notes • *Cisco IP Telephony Operating System, SQL Server, Security Updates*	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Virtual Network Computing (VNC) documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Operating system upgrade executable/support patches and corresponding readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **Note** The operating system and SQL Server support patches post on the voice products operating system cryptographic software page. You can navigate to the site from the voice application (Cisco Unified CallManager, CRS, and so on) software page.
Cisco Security Agent (CSA) and McAfee documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm
Related Cisco Unified Communications application documentation	http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm
Cisco Unity documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/index.htm
Cisco Unified CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Using the Cisco Media Convergence Server Network Teaming Driver	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/driver

What's Changed in This Release

For a list of changes for this release, refer to the *Cisco Unified Communications Operating System Release Notes*. To obtain the document, see Table 2.

Hardware Requirements

For hardware requirements, refer to the *Cisco Unified Communications Operating System Release Notes*. To obtain the document, see Table 2.

Important Considerations

Before you proceed with the operating system installation or software update, review the following recommendations and information:

- Cisco labels new installations of the operating system as either 2000.4.3 or 2000.4.3a, and Cisco labels the operating system upgrade as 2000.4.3a. For some details about 2000.4.3 and 2000.4.3a, review the following information:
  - The Cisco MCS-7825-H2 only supports new installations of 2000.4.3a (not 2000.4.3). All other servers that are listed in the release notes support new installations of 2000.4.3 or 2000.4.3a. To obtain the release notes, see Table 2.
  - If you are performing a new installation and want to identify the version of the operating system installation that your server supports, locate the operating system installation disk that ships in your software kit.
  - If you run 2000.4.3 on the Cisco MCS-7815-I2, Cisco strongly recommends that you apply a 2000.4.3a service release, for example, 2000.4.3asr1, as described in the "Installing Operating System Software Updates" section on page 26. For this server, operating system 2000.4.3 lacks a driver for the PCI-X card, which the 2000.4.3a service release includes.
  - If the server runs 2000.4.3, you cannot upgrade it to 2000.4.3a, but you can apply the 2000.4.3a service releases to get the fixes that are available in 2000.4.3a.
  - You can upgrade any Cisco MCS or Cisco-approved, customer-provided server that runs 2000.2.7 (or later) to 2000.4.3a, unless the server already runs 2000.4.3. The upgrade detects the current version that runs on the server, and if the server does not run a compatible version, the upgrade aborts.
  - The readme document that posts next to the 2000.4.3a upgrade executable provides additional details about the upgrade. To obtain the document, see Table 2.
- This Cisco Unified Communications operating system requires a minimum of 2 GB of memory on the server. If the installation process detects less than 2 GB memory on the server, the installation aborts.
- Install the operating system image on the Cisco Unified CallManager publisher database server first and then on the subscriber server(s).
- Install the same operating system version including the latest operating system service release on all the servers in a cluster.
- Do not configure any server in the cluster as a Windows Domain Controller.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.
- Make sure that you enter the same administrator password on all servers in the cluster.
- Do not attempt to perform any configuration tasks during the installation.
- Install Cisco Security Agent to protect your servers against unauthorized intrusion.

- Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.
- Carefully read the instructions that follow before you proceed with the installation.
- The Ephemeral (Dynamic) port range in operating system version 2000.4.2 specifies 49152–65534 instead of the Windows 2000 default of 1024–4999.
- To protect the server from virus attacks during the operating system installation, complete the operating system installation and apply the latest operating system upgrades and service releases before you connect the server to the network.
- Before you install the software, place the server in a workgroup.
- The system provides support for a limited set of applications where Cisco Unified CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.
- Always disable third-party, Cisco-verified applications on the server before the installation, except when you are installing the operating system for the first time.
- Before you perform the installation, review the "Frequently Asked Questions About the Operating System Installation" section on page 7.

Frequently Asked Questions About the Operating System Installation

Review the following questions and responses before you perform the operating system installation.

What hardware and disks do I receive when I purchase a Cisco MCS or a Cisco Unified Communications application?

You do not receive a monitor, keyboard, or mouse with any Cisco Media Convergence Server (MCS). During initial startup and configuration of the server, you must supply a monitor, a keyboard, and a mouse.

Before you begin the installation, carefully review the hardware documentation that accompanies your server. Make sure that you have the appropriate hardware before installing the operating system. See Table 2 on page 5 for references to server hardware specifications.

Note Unless otherwise specified, this document uses base server model numbers. For example, references to the MCS-7825 apply to servers including the MCS-7825H1, the MCS-7825I1, the customer-provided HP DL320 G3, and the customer-provided IBM xSeries 306.

All Cisco MCS and customer-provided servers that meet approved Cisco configuration standards ship with a blank hard drive. When you purchase a Cisco Unified Communications application, you receive an operating system installation disk and another installation disk for the Cisco Unified Communications application.

Can I install this version of the Cisco Unified Communications Server operating system on any Cisco MCS?

No. This installation supports a new installation on the Cisco MCS, HP servers, and IBM servers that are listed in the operating system release notes. To obtain the release notes, see Table 2.

The installation displays a message if it detects an unsupported server.

How long does it take to perform the operating system installation?

The entire operating system installation process, excluding preinstallation tasks, takes approximately 20 to 30 minutes per server, depending on your server type.

Which Cisco Unified Communications applications use the Cisco Unified Communications operating system?

After you install the Cisco Unified Communications operating system, you install supported Cisco Unified Communications applications on a server that is dedicated solely to the single application or a server that supports coresident applications. The following list provides the Cisco Unified Communications applications that are intended specifically for use with this operating system:

- Cisco Unified CallManager or Cisco CallManager (not Cisco Unified CallManager 5.0)

  Install on a server that is dedicated to the application or install on a server with Cisco Unified CallManager and a supported coresident application.
- Cisco Unified Contact Center Express or Cisco Unified IP-IVR

  Install on a server that is dedicated to the application or install on a server with Cisco Unified CallManager and a supported coresident application.
- Cisco Unified IP Queue Manager
- Cisco Unified MeetingPlace Express
- Cisco Personal Assistant
- Cisco Emergency Responder
- Cisco Conference Connection
- Cisco Unified Customer Voice Portal

Note Cisco Unity does not use the operating system that is represented in this document. Refer to the Cisco Unity documentation for information on the Cisco Unity operating system. See Table 2.

How does the operating system installation work?

When you begin the installation, you boot the server from the operating system installation disk. After the system boots, the installation utility loads automatically and guides you through the installation process; likewise, the utility performs several preinstallation tasks that include preparing your server hard drive and loading server configuration information. (See "What data must I provide to configure the server?" section on page 9 for more information.)

If necessary, the utility upgrades your system BIOS to a recommended version. The installation then automatically installs Microsoft Windows 2000 Server, which is intended solely for use with the Cisco Unified Communications applications. This operating system does not fully function for general use.

What data must I provide to configure the server?

During the installation process, you receive prompts that tell you to enter important configuration information about the server, such as the server name and IP address. You can complete the initial power up more efficiently if you gather all the necessary configuration information before beginning the installation process. The following information applies:

User and Organization Name

Registering the software product that you are installing requires user and organization name. Do not leave the field blank. You can enter underscores, hyphens, numbers, and letters.

Computer Name

Caution Failure to adhere to the described naming convention will result in an inoperable Cisco Unified CallManager system and a complete loss of configuration information and data on a Cisco Unified CallManager publisher database server.

The host name (computer name) for a Cisco Unified CallManager server cannot start with a digit. When you choose a host name that begins with a digit, a Cisco Unified CallManager server does not function properly.

Ensure that the computer name comprises a unique network name of 15 characters or less. It may contain alphanumeric characters and hyphens (-) and must begin with an alphabetical character. Make sure that the computer name and workgroup labels follow the rules for ARPANET host names.

Although Microsoft allows the use of the underscore character (_) as part of the naming convention, Cisco strongly recommends that you do not use the underscore character in the hostname for this computer. The format for DNS domain names comprises labels that are separated by single dots. Each label comprises 1 to 63 characters with a maximum of 255 characters, including the separating dots, for the entire domain name. Labels must adhere to the following naming conventions:

- Ensure that the computer name starts with a letter.
- Ensure that the computer name ends with a letter or digit.
- Ensure that the interior characters of the computer name contain only letters, digits, and hyphens.
- Ensure that the computer name is unique to your network.
- Ensure that the computer name is a maximum of 15 characters.

- Do not include a space anywhere in the computer name, including leading or trailing spaces. Do not use the following characters and symbols, which are not valid entries in computer names: \ " / [ ] : | < > + = ; , ?.

Be aware that the labels are case insensitive and must begin and end with a letter or digit character. Do not create domain names that contain digits only.

Note For unsupported cases, a message warns that the DNS implementation may not support UTF-8 or underscore characters; for example, a message may display when you modify the hostname or DNS suffix and enter a DNS name that includes UTF-8 or underscore character that is not listed in RFC 1123.

If you change the computer name after the application installation, you must reinstall the operating system and the application.

Workgroup

This entry specifies the name of the workgroup to which this computer belongs. A workgroup comprises a collection of computers that have the same workgroup name. Ensure that this entry of 15 characters or less follows the same naming conventions as the computer name. A message displays if you attempt to use the same name for the computer name and workgroup name.

Note Cisco strongly recommends that the server belongs to a workgroup before you install the application. You can change the choice after the installation, but you must place the server in a workgroup again before you upgrade any applications.

Domain Suffix

Always enter the Domain Name System (DNS) domain suffix in the format “mydomain.com” or “mycompany.mydomain.com.” Cisco applications such as Cisco Unified CallManager depend on DNS for resolution between the IP address to host name and vice versa. If your company does not support internet name resolution with a DNS server, enter a fictitious domain suffix such as “mydomain.com” or “mycompany.mydomain.com” during installation and use the same domain suffix when you configure your DNS server.

TCP/IP Properties

Assign an IP address, subnet mask, and default gateway.

Note Cisco recommends that you choose static IP information, which ensures that the server obtains a fixed IP address. With this choice, Cisco Unified IP Phones can register with the application when you plug the phones into the network.

Caution If you choose to use Dynamic Host Configuration Protocol (DHCP), Cisco Technical Assistance Center (TAC) requires that you reserve an IP address for each server in the DHCP server scope. This action prevents the release or reassignment of IP addresses. If you do not reserve IP addresses through the DHCP server scope, the DHCP server may assign a different address to the server if the server is disconnected from, and then reconnected to, the network. To return the server to its original IP address, you must reprogram the IP addresses of the other devices on the network.

You cannot provision the IP address on this server by using the DHCP server that is provided with this operating system. You must use a separate DHCP server to assign a reserve IP address to this server. For more information on DHCP and how to configure the DHCP server that is provided with this operating system, press **F1** to access the Microsoft Windows 2000 Server online help after you complete the operating system installation.

Domain Name System (DNS)

The Cisco Unified Communications application that you install may require you to configure DNS or some type of NetBIOS/IP (NetBIOS over IP) name resolution such as Windows Internet Name Service (WINS). Cisco Unified CallManager requires both DNS and NetBIOS name resolution. You can configure a separate Microsoft WINS server, configure LMHOSTS files on each server, or enable the DNS server that is provided with this operating system. For more information on DNS, WINS, LMHOSTS and on how to enable the DNS server that is provided with this operating system, press **F1** to access the Microsoft Windows 2000 Server online help after you complete the operating system installation.

Note Cisco does not recommend using LMHOSTS for name resolution when more than 10 nodes exist in your network.

Caution You must have a name resolution method in place, such as Domain Name System (DNS), Windows Internet Name Server (WINS), or local naming that uses a configured LMHOSTS file. If you use DNS, make sure that the DNS server contains a mapping of the IP address and hostname of the server that you are installing before you begin the installation. If you use local name resolution, ensure that the LMHOSTS file is updated on the existing servers in the cluster before you begin the installation on the subscriber server; then, you must add the same information to the lmhosts file on the new server during installation, as the procedure instructs.

NT Administrator Password

You must enter and confirm an administrator password. Cisco requires a password for security purposes. If you leave the password blank, you cannot install a Cisco Unified Communications application on the server.

Tip Ensure that you use the same administrator password on all servers in the cluster.

Configuration Data

See Table 3 on page 12 for configuration information that is required for installing the operating system on your server.

- Complete all fields unless otherwise noted.
- Gather this information for each Cisco Unified Communications Server that you are installing in the cluster.
- Make copies of this table and record your entries for each server in a separate table.
- Before you begin the installation, obtain the configuration data.

Table 3 Configuration Data for Cisco Unified Communications Servers

Configuration Data	Your Entry
User name Name of your Organization	
Computer name Administrator Password	
Current date, time, and time zone	
TCP/IP properties (required if you choose custom network configuration) • IP address • Subnet mask • Default gateway	
DNS servers • Primary • Alternate DNS domain suffix WINS servers • Primary • Secondary LMHosts file	You must have a name resolution method in place, such as Domain Name System (DNS), Windows Internet Name Server (WINS), or local naming that uses a configured LMHOSTS file.
Workgroup	During the operating system installation, Cisco requires that you configure the server in a workgroup.
NT domain (optional)	

Which Cisco-verified, third-party applications may I install on the server?

Caution Cisco supports a limited list of applications on the servers where Cisco Unified CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.

To review a list of third-party, Cisco-verified applications that you may install on the server, perform the following procedure:

Procedure

Step 1 Click http://www.cisco.com/pcgi-bin/ecoa/Search.

Step 2 In the Solution drop-down list box, click **IP Communications**.

Step 3 From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**.

Step 4 If you want to do so, choose a company.

Step 5 Click **Search**.

Caution Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.

Must I disable Cisco-verified applications?

Except for the first operating system installation, you must disable Cisco Security Agent as well as any third-party, Cisco-verified applications on your servers whenever you perform a reinstallation or upgrade of the operating system.

Caution To successfully complete installation, upgrade, or restoration procedures, you must disable and stop all Cisco-verified applications/services on every server in the cluster.

To disable services, choose **Start > Settings > Control Panel > Administrative Tools > Services**. From the Services window, right-click the service and click **Properties**. Click the drop-down arrow for the Startup-type field and choose **Disabled**. Click **Stop**; then, click **OK**.

Disabling and stopping platform agents and services, such as Cisco Security Agent, performance monitoring (for example, NetIQ), antivirus service (for example, Cisco-verified McAfee services), and remote management services, ensure that the installation does not encounter issues that are associated with these services.

Which Cisco Unified Communications applications may I install on the same server as Cisco Unified CallManager?

Consider the following information before you install other software besides Cisco Unified CallManager on the Cisco MCS or the Cisco-approved, customer-provided server:

- The system does not support Cisco Unity on a server that runs this version of the operating system.
- To identify the Cisco Unified Communications applications that you can install on the Cisco Unified CallManager server, see "Which Cisco Unified Communications applications use the Cisco Unified Communications operating system?" section on page 8.
- Cisco strongly recommends that you install a security agent to protect your servers against unauthorized intrusion. Cisco offers the following security agent options: Cisco Security Agent (CSA) for Unified CallManager and Management Center for Cisco Security Agent (CSA MC).

  CSA for Cisco Unified CallManager comprises a standalone agent and security policy that is designed to be used on all servers in the voice cluster. Because the policy that this agent includes is configured specifically for Cisco Unified CallManager and other Cisco Unified Communications applications, you cannot update or view it. You can download the agent from

  http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des.

  If you want to add, change, delete, or view rules and policies that CSA for Cisco Unified CallManager includes, or if you want to add support for non-Cisco approved, third-party applications, you must purchase and install the fully managed console, CSA MC. CSA MC requires a separate, dedicated server to be used as the management center. This management center allows you to create agent kits that are then distributed to agents that are installed on other network systems and servers.

  To access information on Cisco Security Agent, see Table 2 on page 5.

Caution If you are uncertain whether a Cisco Unified Communications application is supported on the server, do not install it. Before you install the application, always review the application documentation for recommended configurations and installations.

May I run a web browser on the server?

Cisco strongly recommends that you do not run a web browser on the Cisco MCS or a Cisco-approved, customer-provided server. Cisco approved, customer-provided servers must adhere to exact server configurations. See Table 2 for references to documents on server hardware specification.

Running a web browser on the server causes CPU usage to surge; access the server by using a web browser from another computer on the same network.

May I use Terminal Services, VNC, or ILO to install the operating system on this server?

About Terminal Services

Cisco does not support installations or upgrades through Terminal Services.

Caution Before a software update, for example, an upgrade, Cisco strongly recommends that you disable Terminal Services and immediately reboot the server to prevent remote access to the server. Accessing the server via Terminal Services may cause the software update to fail.

After you update the server, you must enable Terminal Services.

About Virtual Network Computing

If you want to use Virtual Network Computing (VNC) to remotely install supported applications, see Table 2 to obtain the latest version of the VNC document.

Caution If you installed VNC but do not plan to use it, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the software update, for example, the operating system upgrade, the update fails.

About Integrated Lights Out (ILO)

HP servers support Integrated Lights Out (ILO). If your server is a Cisco MCS (HP equivalent; for example, MCS-7835H-2.4) or Cisco-approved, customer-provided HP server, you can use ILO for remote configuration and monitoring tasks. Cisco does not support ILO for any other purposes, including installation and upgrade tasks. Cisco supports the following standard features of ILO:

- Virtual Power to allow full remote control of the server power button
- Remote text console to enable the display and control of remote host server activities such as shutdown and startup

To use ILO, you must obtain the ILO Default Network Settings tag that shipped with your server and perform all necessary startup tasks. Refer to the documentation that accompanies your hardware.

The ILO administrator who accesses the remote server controls all tasks that occur on the server. If an administrator is performing an installation/upgrade directly on the server and the ILO administrator tries to access the server, the ILO administrator controls all tasks on the server. These tasks may interrupt the installation or upgrade; to prevent interruptions, notify all users who can access the server before the upgrade occurs. When an ILO administrator accesses a remote server, the application locks the keyboard and mouse on the remote server where the tasks are occurring.

May I configure a server in the cluster as a Domain Controller?

Do not configure any server in the cluster as a Domain Controller. If you configure any server in the cluster as a Domain Controller, you cannot upgrade or reinstall Cisco Unified CallManager on the server.

What preinstallation tasks should I perform?

For preinstallation tasks that you must complete before you install this operating system, see Table 4.

Table 4 Preinstallation Tasks

	Preinstallation Tasks	Important Notes
Step 1	Carefully review the hardware documentation that accompanies your server. Make sure that you have the appropriate hardware before installing the application.	To obtain the server hardware specifications, see Table 2.
Step 2	Connect a monitor, keyboard, and mouse to the server.	See the "How do I connect the keyboard and mouse to the server?" section on page 16.
Step 3	Locate Table 3, which provides specific server configuration information.	See the "What data must I provide to configure the server?" section on page 9.

What post-installation tasks should I perform?

For post-installation tasks that you must complete before you install the Cisco Unified Communications application, see Table 5 on page 19.

How do I connect the keyboard and mouse to the server?

You must supply a monitor and, if necessary, a keyboard and mouse to use during initial startup and configuration of the server.

Plug the mouse and keyboard into the standard mouse and keyboard connectors that are marked on the back of the server. Plug the monitor cable into the monitor connector on the back of the server.

Caution When installing the operating system on the Cisco MCS, you must use a legacy PS/2 mouse and keyboard. If you use a USB keyboard or mouse, the operating system may not install successfully.

Note If you connect a MCS server to a Raritan Keyboard/Video/Mouse (KVM) switch, the keyboard and mouse may not work properly. You need a hardware fix for the KVM switch, so contact Raritan directly.

What if I encounter problems during the installation?

Take the following actions if you encounter problems during the installation:

1. During the installation, if you receive a message that displays in a dialog box, see the "Error Messages" section on page 28 and perform the recommended corrective action.
2. If you perform a new installation, obtain and review the MCSSetup.log log file, which you can access by navigating to the following folder on the server where the problem occurred: **C:\Program Files\Common Files\Cisco\Logs**.

Note Be aware that not all messages that display in the log file are catastrophic. Messages appear in the log file for many reasons. For example, messages show attempts to access a service that Cisco Unified CallManager does not use.

Where do I obtain the release notes?

To obtain the release notes, see Table 2 on page 5.

Installing the Operating System

Caution Before the installation, be aware that the process erases the server hard drive and all data and configuration information, if present. If you are reinstalling the operating system and you want to retain the present configuration, be sure to record your previous configuration settings.

Note During the installation, the server reboots several times. Do not power off the server at any time during this process, unless instructed. Any unexpected power interruption during the installation process may prevent proper completion of the configuration and may prevent the operating system from restarting.

Before you connect your server to the network, install the latest operating system upgrade and apply the appropriate Microsoft hotfixes.

To protect the server from virus attacks during the operating system installation, Cisco recommends that you complete the operating system installation and apply the latest operating system upgrades and service releases before you connect the server to the network.

During the installation, you perform the following tasks:

- Insert the operating system installation disk into the drive.
- Click to acknowledge that the installation process erases existing data.
- Read and agree to the terms in the End User License Agreement.
- Enter your user name and name of your organization.
- Enter the computer name and the administrator password.
- Choose the appropriate time zone, date, and time.
- Choose the network setting configuration.
- Join a workgroup, which serves as a requirement for the application installation.

Using the data that you collected in Table 3, complete the following procedure to configure each server:

Note The server may reboot multiple times to complete installation of additional drivers and patches. Do not reboot the system manually during this time, unless the installation instructs you to do so.

Procedure

Step 1 Locate the operating system installation disk.

Step 2 Insert the disk and then power up the server. You must boot from this disk to begin installing the operating system.

Tip The first time that you start up a new server, you do not see any indication that the startup process is operating normally. The startup on a new server takes longer than on preinstalled servers. You may wait as long as 3 minutes before a video connection occurs.

Do not remove the disk unless the procedure or process prompts you to do so.

Step 3 When a message displays that states that all existing configuration and information on the hard drive will be lost, click **OK** to continue the installation.

Step 4 A message that states that the installation is transferring the operating system image to the server displays. This process takes approximately 15 minutes. You can either click **OK** or wait for the installation program to start transferring the image by showing the percentage that is complete. The system reboots automatically after the image transfer completes.

Step 5 The License Agreement window displays. Read through the contents of the agreement. To continue the installation, you must click **I Accept this agreement**; then, click **Next**.

Step 6 The Personalize Your Software window displays. Enter your name and the name of your company or organization. Click **Next**.

Step 7 The Computer Name and Administrator Password window displays. Enter the computer name in the computer name field and the administrator password in the administrator password field. Enter the same password in the Confirm Password field. Click **Next**.

Caution Failure to adhere to the naming convention for computer names results in an inoperable Cisco Unified CallManager system and a loss of configuration and data on the Cisco Unified CallManager publisher database server. For information on the naming convention, see the "Computer Name" section on page 9.

Tip If you leave the password fields blank, you cannot install any Cisco Unified Communications applications on the server. To ensure that you enter the appropriate password, verify the Num Lock status before you enter the password. Make sure that you enter the same password on all servers in the cluster.

The installation automatically enables screen saver password protection. You can disable the screen saver password protection by unchecking the Password-protected check box on the screen saver tab in the Display Property Configuration window.

Step 8 The Date and Time Settings window displays. Set the current date and time. Choose the appropriate time zone. To adjust the time zone for daylight saving time, check the check box in the Time Zone pane. Click **Next**.

Step 9 The Workgroup or Computer Domain windows display. If the server exists in a domain, Cisco requires that you place the server in a workgroup during the installation. To join a workgroup, perform the following procedure:

a. Click the **No, this computer is not on a network, or is on a network without a domain** radio button.

b. Enter a name of the workgroup, for example, WRKGRP. Make sure that you enter a workgroup name that differs from the computer name.

c. Click **Next**.

Step 10 After the installation completes, the server reboots. Log in to the server by using the administrative user name and password.

Step 11 The system checks for network transmission conflicts the first time that the server is started after the operating system is installed. If your server displays a message to this effect, click **OK** to remove the message. If you received an error message, correct the network conflict that the installation program detected, clear the System log under Event Viewer, and rerun the utility CheckNICDuplex.exe in the C:\utils folder to ensure that no more network conflicts exist.

Step 12 Install the operating system on every server in the cluster.

Step 13 After you complete the installation, configure network settings on each server in the cluster, as described in the "Configuring Network Settings" section on page 20.

Step 14 Refer to the Cisco Unified Communications application documentation for additional installation and configuration tasks. See Table 2 on page 5.

Performing Post-Installation Tasks

See Table 5 for a list of tasks that you should perform after you install the operating system software.

Table 5 Post-Installation Tasks

Task	Notes
Configure network settings.	See the "Configuring Network Settings" section on page 20. See the "What data must I provide to configure the server?" section on page 9
Verify the operating system version that is installed on the server.	See the "Verifying the Operating System Version" section on page 22.
Verify that you have all hotfixes and support patches installed on the server. If not, download and install the latest operating system service release that is available on the web.	See Table 2 on page 5 for a reference to the readme document for the operating system support software. See the following sections: • Frequently Asked Questions About Operating System Software Updates, page 24 • Installing Operating System Software Updates, page 26

Table 5 Post-Installation Tasks (continued)

Task	Notes
If you plan to install Cisco CallManager Release 3.3(2) or 3.3(3), uninstall the non-security Microsoft hotfix 831877 that the operating system includes.	See the "Uninstalling Microsoft Hotfix 831877" section on page 22.
Subscribe to the Cisco Unified CallManager Notification Tool and PSIRT notification tool.	This task enables you to receive e-mail notification whenever new fixes, operating system updates, and service releases become available. See the "Applying Additional Security" section on page 23.
Increase the security on your server.	See the "Applying Additional Security" section on page 23.
If your hardware supports network teaming (HP only), enable the Cisco Media Convergence Server (MCS) Network Teaming Driver to support the functionality for the failover, fault-tolerant network adapters.	Refer to *Using the Cisco Media Convergence Server Network Teaming Driver* for a list of supported servers and installation information.
Configure the speed and duplex of your network card to 1000/Full if the hardware on your server and network supports gigabit speed.	Refer to *Using the Cisco Media Convergence Server Network Teaming Driver.*

Configuring Network Settings

Tip Cisco recommends that you configure static IP information, which ensures that the Cisco Unified CallManager server obtains a fixed IP address. With this choice, Cisco Unified IP Phones can register with Cisco Unified CallManager when you plug the phones into the network.

If you choose to use Dynamic Host Configuration Protocol (DHCP), Cisco Technical Assistance Center (TAC) requires that you reserve an IP address for each server in the DHCP server scope. This action prevents the release or reassignment of IP addresses. If you do not reserve IP addresses through the DHCP server scope, the DHCP server may assign a different address to the server if the server is disconnected from, and then reconnected to, the network. To return the server to its original IP address, you must reprogram the IP addresses of the other devices on the network.

For other information on configuring network settings, see the "What data must I provide to configure the server?" section on page 9.

To configure network settings on the server, perform the following procedure:

Procedure

Step 1 On the desktop, right click **My Network Connections** and choose **Properties**.

Step 2 Although the server comes with two Network Interface Cards (NIC), Cisco recommends that you configure the network settings on the first NIC. To configure network settings on the first NIC on the server, click **Internet Protocol (TCP/IP)**; then, click **Properties**.

Tip Cisco strongly recommends that you configure a static IP address instead of using DHCP. For more information on DHCP and static IP addresses, see the "What data must I provide to configure the server?" section on page 9.

Step 3 To configure static IP information, click **Use the following IP address**; in the appropriate fields, enter the server IP address, subnet mask, and default gateway, as described in the "What data must I provide to configure the server?" section on page 9.

Step 4 To use DHCP, click **Obtain the IP address automatically**.

Caution You must have a name resolution method in place. If you do not plan to use DNS, you must configure WINS or configure local name resolution by updating the LMHOSTS file with IP address and hostname information for every server in your cluster.

If you do not plan to configure DNS, leave the DNS fields empty in the Internet Protocol (TCP/IP) Properties window. Make sure that the radio button, Use the following DNS server addresses, is not chosen, so you can configure WINS or local name resolution; to configure WINS, see Step 6. To configure LMHOSTS file, see Step 7.

To Configure DNS

Step 5 In the Internet Protocol (TCP/IP) Properties window, click the **Use the following DNS server addresses** radio button; then, enter the IP addresses of the primary and alternate DNS servers. Click **OK**.

To Configure WINS

Step 6 To configure WINS, perform the following procedure:

a. In the Internet Protocol (TCP/IP) Properties window, click the **Advanced** button.

b. Click the **WINS** tab.

c. Click the **Add** button.

d. Enter the WINS server address.

e. Click **Add**.

f. To add additional server addresses, repeat Step 6.

g. After you complete Step 6 for all addresses that you want to add, click **OK**.

To Update the LMHOSTS File

Step 7 If you did not configure DNS or WINS server information, and if you are installing multiple servers in a cluster, you must configure local name resolution by updating the LMHOSTS file, so it contains a mapping of the IP address and hostname of each server in the cluster. To update the LMHOSTS file, perform the following steps:

a. On the server that runs this operating system, choose **Start > Run**.

b. In the Open field, enter **command**; click **OK**.

c. At the DOS prompt, enter **notepad c:\winnt\system32\drivers\etc\hosts**.

The file opens.

d. On a new line at the end of the hosts file, enter the following information in two different columns: IP address of the server (first column) and Cisco Unified CallManager server name (second column).

Tip Make sure that you enter at least one space between the IP address and the server name.

For example, the IP address for the publisher database server equals 171.16.1.251 and the Cisco Unified CallManager server name equals ccm1. On a new line at the end of the hosts file, the administrator enters the IP address and server name in different columns and includes at least one space between the data.

```
171.16.1.251          ccm1
```

e. Save the file and close NotePad.

Step 8 Perform the procedure on each server in the cluster.

Verifying the Operating System Version

The MCSver.exe program reports the current version of the operating system components. Be aware that Cisco does not report the actual application version through this program. Most of these components, which are run from the installation disks during the initial installation, no longer exist on the system.

The version for the operating system image equals your operating system disk version number. The version for the operating system upgrade equals the version of the operating system upgrade that you last ran either via upgrade disk (if available) or via the web.

Perform the following procedure to view the operating system versions that are installed on the server:

Procedure

Step 1 On your server, choose **Start > Cisco OS Version** to verify the operating system image version that runs on your server.

Step 2 Locate the operating system image version and the operating system upgrade version.

Note The Cisco OS Version utility, named MCSver.exe, logs information to C:\Program Files\Common Files\Cisco\Logs\MCSver.log. If necessary, you can provide log files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

Uninstalling Microsoft Hotfix 831877

If you are planning to install Cisco CallManager Release 3.3(2) or 3.3(3), you may encounter a problem during installation in which the Cisco CallManager installation program displays a harmless AddAnonymousWebUserAccess message.   Click **OK** to continue your installation.

You must uninstall the non-security Microsoft Windows hotfix 831877 that Cisco Win-OS 2000.4.1 (and later) includes.

Note Microsoft Windows hotfix 831877 comprises a non-security update that is reapplied when you install a Cisco Win-OS service release.

Procedure

Step 1 From the Start menu, choose **Settings** > **Control Panel**.

The Control Panel window displays.

Step 2 Double-click the Add/Remove Programs icon.

The Add/Remove Programs window displays.

Step 3 Scroll until you locate the Windows 2000 Hotfix 831877 and click the hotfix.

Step 4 Click **Change/Remove**.

Applying Additional Security

Cisco recommends that you perform the following additional tasks on all servers in a cluster:

- Always apply the latest operating system upgrades and service releases.
- Install a Cisco-verified antivirus program on all servers.
- Cisco strongly recommends that you install Cisco Security Agent to protect your servers against unauthorized intrusion. Refer to the Cisco Security Agent documentation. See Table 2 on page 5.
- If you plan to install Cisco Unified CallManager, you can install the Cisco Unified CallManager OS Optional Security settings. For more information, refer to C:\Utils\SecurityTemplates\CCM-OS-OptionalSecurity-Readme.htm.
- Subscribe to the Cisco Unified CallManager Notification Tool and PSIRT notification tool.

  The Cisco Unified CallManager Notification Tool provides automatic e-mail notification of new fixes, operating system updates, and service releases that are available for Cisco Unified CallManager and related products, including Cisco Unified CallManager Attendant Console, Cisco Unified CallManager Assistant, or Bulk Administration Tool (BAT). To subscribe, click the following URL and choose **CallManager Cryptographic Software including OS updates** to receive notification when new operating system updates are posted. (Only a registered user of Cisco.com can access this URL.)
  http://www.cisco.com/cgi-bin/Software/Newsbuilder/Builder/VOICE.cgi

  The Cisco PSIRT Advisory Notification Tool provides automatic e-mail notification of all Cisco Security Advisories that the Cisco Product Security Incident Response Team (PSIRT) releases. Security Advisories, which describe security issues that directly impact Cisco products, provide a set of required actions to repair these products. To subscribe, click the following URL and perform the tasks as directed:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Frequently Asked Questions About Operating System Software Updates

Review the following information before you upgrade the operating system.

Why can I not find the web executable that the Cisco Unified Communications application documentation specifies?

If you cannot locate a file on Cisco.com, Cisco removed the file from the web and replaced it with a newer version. Always install the version that is available on the web, unless the readme document states otherwise.

In what order should I apply the software updates?

Refer to *Cisco IP Telephony Operating System, SQL Server, Security Updates* for more information. See Table 2 to obtain the document.

How long does it take to upgrade the operating system?

The upgrade takes approximately 20-60 minutes, depending on the server type, the speed of the hardware, and the age of the components (BIOS, and so on).

Where do I find more information (release notes/readme) about the software update?

You can obtain the latest upgrade executable and version-specific readme document from the voice software cryptographic site on Cisco.com.

Be aware that the readme document may be a later version than the executable. Cisco recommends that you review the updated document for new information regarding the upgrade.

When should I install the software update?

Caution Cisco strongly recommends that you install the software update during off-peak hours or a maintenance window. Installing the software update may cause call-processing interruptions.

Which versions of the operating system are compatible with operating system upgrade 2000.4.3a?

You can upgrade any Cisco MCS or Cisco-approved, customer-provided server that runs 2000.2.7 (or later) to 2000.4.3a, unless the server already runs 2000.4.3. The upgrade detects the current version that runs on the server; if the server does not run a compatible version, the upgrade aborts. If the server runs 2000.4.3, you cannot upgrade it to 2000.4.3a, but you can apply the 2000.4.3a service releases to get the fixes that are available in 2000.4.3a.

For other important considerations, see the "Important Considerations" section on page 6.

May I perform configuration tasks during the update?

Caution Do not attempt to perform any configuration tasks during the installation. Before you update the server, disable all services that allow any administrator to perform remote configuration tasks. For example, disable Terminal Services or VNC, if you do not plan to use it, before the upgrade to prevent an administrator from browsing into the server during the installation.

Notify all users that you are performing an installation, so users do not browse into the server.

Performing configuration tasks during the installation causes an installation failure.

May I use Terminal Services, VNC, or ILO on this server during an update?

Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote administration and troubleshooting tasks. Cisco does not support operating system installations, upgrades, or software updates through Terminal Services.

Caution Before the update, Cisco strongly recommends that you disable Terminal Services and immediately reboot the server to prevent remote access to the server. Accessing the server via Terminal Services may cause the update to fail. After you perform the update, you must enable Terminal Services.

If you want to use Virtual Network Computing (VNC) to remotely install supported applications, see Table 2 on page 5 to obtain the latest version of the VNC document.

Caution If you installed VNC but do not plan to use it to perform the update, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the update, the update fails.

HP servers support Integrated Lights Out (ILO). If your server is a Cisco MCS (HP equivalent; for example, MCS-7835H-2.4) or Cisco-approved, customer-provided HP server, you can use ILO for remote configuration and monitoring tasks. Cisco does not support ILO for any other purposes, including installation and upgrade tasks.

To use ILO, you must obtain the ILO Default Network Settings tag that shipped with your server and perform all necessary startup tasks. To use this product, refer to the documentation that accompanies your hardware.

The ILO administrator who accesses the remote server controls all tasks that occur on the server. If an administrator is performing an installation/upgrade directly on the server and ILO administrator tries to access the server, the ILO administrator controls all tasks on the server. When an ILO administrator accesses a remote server, the application locks the keyboard and mouse on the remote server where the tasks are occurring. These tasks may interrupt the installation or upgrade; to prevent interruptions, notify all users that can access the server regarding when the upgrade will occur.

What pre-/post-update tasks should I perform?

See the "Installing Operating System Software Updates" section on page 26.

What if I encounter problems during the operating system upgrade?

If you encounter problems during the installation, Cisco recommends that you take the following actions:

1. If you receive a message that displays in a dialog box during the operating system upgrade, see the "Error Messages" section on page 28 and perform the recommended corrective action.
2. On the server where the upgrade problem occurred, obtain and review the log file, MCSOSupg.log, from C:\Program Files\Common Files\Cisco\Logs.

Note Be aware that not all messages that display in the log file are catastrophic. Error messages display in the log file for many reasons; for example, attempts to access a service that Cisco Unified CallManager does not use display.

Installing Operating System Software Updates

This section describes how to download and install operating system upgrades, hotfixes, operating system service releases, and additional operating system software updates from Cisco.com.

The operating system upgrade updates your system to the latest Cisco Unified Communications operating system version. Do not perform the operating system upgrade on a server that is already running the same version of the operating system.

Perform updates on the Cisco Unified CallManager publisher database server first and then on the subscriber server(s) one at a time.

Before You Begin

- Verify that the server runs a compatible version of the operating system, as described in the "Which versions of the operating system are compatible with operating system upgrade 2000.4.3a?" section on page 25.
- Disable all Cisco-verified, third-party applications and reboot the server.
- Disable Cisco IDS Host Sensor Agents and reboot the server.
- Verify that you installed the latest backup utility that is available on the web. Verify that you have a good backup of your data on a network directory or tape device.

- Verify that you have enough free disk space on the server. Make sure that you have 1 GB of free disk space. Delete any unnecessary files. Remove old log files, CDP records, old installation files, and so on.
- Close all programs.

To install the software update, perform the following procedure:

Procedure

Step 1 Before you install the software update, review the "Frequently Asked Questions About Operating System Software Updates" section on page 24.

Step 2 Click http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des.

Note To obtain the update from the web, you must log in with your Cisco Connection Online (CCO) username and password.

Step 3 In the window that displays, locate the readme document for the software update.

Step 4 Review the readme document for specific installation procedures, notes, caveats, and compatibility information.

Step 5 Download the software update to your hard drive.

Step 6 Keep track of the location where you save the downloaded file.

Step 7 To begin the installation, double-click the downloaded file.

Step 8 Perform the installation on every server where the update is supported, starting with the Cisco Unified CallManager publisher database server followed by the subscriber servers one at a time.

Step 9 Perform post-installation tasks, as described in the "Additional Tasks (Post-Update)" section on page 27.

Additional Tasks (Post-Update)

- Enable all Cisco-verified, third-party applications and services that you disabled before the update; reboot the server.
- Verify that the following services are running:
  - MS-SQL Agent, MS-SQL Server, and other SQL dependencies
  - DC Directory
  - SNMP and its dependencies
  - IIS Admin and its dependencies on the publisher database server
  - Network Time Protocol

Tip If the services are not running, start the services by choosing **Start > Settings > Control Panel > Administrative Tools > Services**. From the Services window, right-click the service and choose **Start**.

- Verify that you can place and receive calls and that all features work as expected. For more information on supported features, refer to the application documentation that support the features; for example, refer to the *Cisco Unified CallManager Features and Services Guide*.

- Verify that all necessary services in Cisco Unified CallManager Serviceability are running on the server. Refer to the *Cisco CallManager Serviceability Administration Guide* (for 3.3) or *Cisco Unified CallManager Serviceability Administration Guide* (for 4.1 and 4.2).

Ongoing Server Management

The HP Insight Management Agent or the IBM Director Agent, both SNMP agent extensions, allow you to monitor and manage the specific components of your server, such as CPU, virtual memory, and disk usage. They also monitor server temperature, fan status, power supplies, and NIC information. On Cisco Media Convergence Servers and Cisco-approved, customer-provided servers, the drivers upgrade when you upgrade the operating system.

Error Messages

Table 6 describes error messages that display in dialog boxes and the appropriate corrective actions. If you need to obtain the log files, see the "What if I encounter problems during the installation?" section on page 16.

Table 6 Error Messages

Error Message	Corrective Action
Any existing configuration and information on the hard drives will be lost. DO YOU WISH TO PROCEED? ALL DATA WILL BE LOST.	To continue the installation, click **OK**.
Configuring the Hard Drives. System will reboot upon completion...	The system automatically configures the hard drives. You do not need to take any action.
Configuring System BIOS.	The system automatically configures the BIOS. You do not need to take any action.
Configuring System BIOS. System will reboot upon completion...	The system automatically configures the BIOS. You do not need to take any action.
Clearing the RAID Array Configuration... Clear RAID Configuration	The system automatically clears the RAID configuration. You do not need to take any action.
The SATA RAID BIOS Setting will be enabled on this system and a reboot is required. The System will now reboot. REBOOT REQUIRED	The system reboots automatically; you do not need to take any action.
Transferring Image on to System. This will take several minutes...	You do not need to take any action.
Image transfer is initiating...	You do not need to take any action.
Elapsed time for Image Transfer is <number> minutes.	The transfer time depends on the server type, interface speed, and other factors. You do not need to take any action.
Adding latest Security and System Updates.	You do not need to take any action.
The installation program has determined that this server is not supported by this media.	This message displays when the server is not associated with the DVD media.

Table 6 Error Messages (continued)

Error Message	Corrective Action
The memory detected was not a minimum expected <number> MB Actual detected memory: <number> MB Please correct before reattempting installation. Memory Size Fatal Error	This message displays when the server does not have the minimum memory. Before you proceed with the installation, increase the memory.
The number of CPUs detected was not the expected <number> count Actual detected CPU count: <number> Please correct before reattempting installation. CPU Count Fatal Error	This message displays when the server does not have the correct number of processors. Before you proceed with the installation, correct the problem.
The CPU speed detected was not the expected <number> MHz. Actual detected CPU speed: <number> MHz Please correct before reattempting installation. CPU Speed Fatal Error	This message displays when the server processors do not have the correct CPU speed. Before you proceed with the installation, correct the problem.
The hard drive size detected was not the expected <number> MB Actual detected size: <number> MB Please correct before reattempting installation Drive Size Fatal Error	This message displays when the size of the physical drives is not the correct value. Before you proceed with the installation, install hard drives that meet the minimum requirements.
The number of hard drives detected was not the expected <number> drive(s) Actual detected number: <number> Please correct before reattempting installation. Drive Size Fatal Error	This message displays when the number of physical drives is not the correct value. Before you proceed with the installation, inspect the drives and correct the number of drives, if required.
Configuring the RAID Array Controller. System will reboot upon completion... Configuring RAID Controller	The system automatically configures the RAID Array Controller and reboots. You do not need to take any action.
The BIOS Version detected is prior to the approved version of: <number> Actual detected version: <number> Please correct before reattempting installation BIOS Version Fatal Error	The installation may not support the system BIOS family. This message may display if the server is not supported. Before you proceed with the installation, correct the problem.

Table 6 Error Messages (continued)

Error Message	Corrective Action
The current version of the BIOS is <number> This BIOS version is below the minimum expected version of <number> The BIOS will be automatically upgraded as part of this installation. Press 'OK' to continue or 'Cancel' to abort the installation. BIOS Version Warning	To continue, click **OK**, and the system upgrades the BIOS to the correct version.
The current version of the BIOS is <number> The BIOS version tested on this system is <number> Please note this system has not been tested with the detected BIOS version of <number> Press 'OK' to continue or 'Cancel' to abort the installation. BIOS Version Warning	The server has a later BIOS than the version that was tested. To continue the installation, click **OK**; the system does not downgrade the BIOS.
The current version of the BIOS is <number> The BIOS version tested on this system is <number> The BIOS will be automatically adjusted as part of this installation. Press 'OK' to continue or 'Cancel' to abort the installation. BIOS Version Warning	The server has a different BIOS than the version that was tested. To continue the installation, click **OK**. The installation automatically upgrades or downgrades the BIOS.
The current version of the RAID Firmware is <number> This RAID Firmware version is below the minimum expected version of <number> The RAID Firmware will be automatically upgraded as part of this installation Press 'OK' to continue or 'Cancel' to abort the installation RAID Firmware Version Warning	This message displays when the RAID firmware on the server represents an earlier release than the version that was tested. To continue the installation, click **OK**. The installation upgrades the RAID firmware to the tested version.

Table 6 Error Messages (continued)

Error Message	Corrective Action
The current version of the RAID Firmware is <number> The RAID Firmware version tested on this system is <number> Please note this system has not been tested with the detected RAID Firmware version of <number> Press 'OK' to continue or 'Cancel' to abort the installation RAID Firmware Version Warning	This message displays when the RAID firmware on the server represents a later release than the version that was tested. To continue the installation, click **OK**. The installation does not downgrade RAID firmware.
The current version of the RAID Firmware is <number> The RAID Firmware version tested on this system is <number> The RAID Firmware will be automatically adjusted as part of this installation. Press 'OK' to continue or 'Cancel' to abort the installation. RAID Firmware Version Warning	This message displays when the RAID firmware on the server represents a different release than the version that was tested. To continue the installation, click **OK**. The installation upgrades or downgrades the RAID firmware to the tested version.
The current version of the RAID BIOS is <number> The RAID BIOS version tested on this system is <number> The RAID BIOS will be automatically adjusted as part of this installation. Press 'OK' to continue or 'Cancel' to abort the installation. RAID BIOS Version Warning	This message displays when the RAID BIOS on the server represents a different release than the version that was tested. To continue the installation, click **OK**. The installation upgrades or downgrades the RAID BIOS to the tested version.
The transfer of the OS image to the hard drive failed! This can be caused by scratched or smudged DVD-ROM media or a hardware failure within the system. Fatal Error	This message displays when the installation cannot properly transfer the operating system to the hard drive. Verify the condition of the DVD media and attempt the installation again.
A failure to program the BIOS was encountered. Error Code: <number> Fatal Error	This message displays when the installation cannot configure the system BIOS. Verify the health of server, and attempt the installation again.

Table 6 Error Messages (continued)

Error Message	Corrective Action
The installation was unable to detect the needed state information! This can be caused by a corrupted or incompatible BIOS version. Error code: <number> Fatal Error	This message displays when the installation cannot determine the necessary state information. Attempt the installation again.
The installation was unable to reset needed state information! This can be caused by a corrupted or incompatible BIOS version. Error code: <number> Fatal Error	This message displays when the installation cannot change the state information. Attempt the installation again.
The installation was unable to retrieve needed system information! Error code: <number> SysInfo Fatal Error	This message displays when the installation cannot determine the necessary system information. Attempt the installation again.
The installation was unable to retrieve needed drive information! Error code: <number> Drive Count Fatal Error	This message displays when the installation cannot determine the number of hard drives. Verify that the hard drives are functioning and properly installed. Attempt the installation again.
The configuration of the array controller failed! This can be caused by unexpected hardware or a hardware failure within the system. Error code: <number> Fatal Error	This message displays when the RAID controller failed to accept the configuration information. Write down the error message in a place that you will remember and attempt the installation again.
The transfer of the latest Security and System Updates failed! This can be caused by scratched or smudged DVD-ROM media or missing files on the DVD-ROM.	An internal error occurred. Attempt the installation again.
The installation will now abort.	This message displays at the end of any fatal error.
OS image complete. Now Rebooting...	You do not need to take any action.

Table 6 Error Messages (continued)

Error Message	Corrective Action
The IBM Director Agent WMI CIM Server service is stopping..... The IBM Director Agent WMI CIM Server service was stopped successfully. System error 1060 has occurred. The specified service does not exist as an installed service. The system cannot find the file specified.	Before the Cisco Unified Communications application installation, the operating system calls the CLR utility, which stops processes that may adversely impact the installation of the Cisco Unified Communications application; if these informational messages display, click **OK** to continue the installation. The 1060 event message indicates that the specified service does not exist on the server; therefore, the utility cannot stop the service.
No NIC duplex mismatch reported in the System Event log.	The CheckNICDuplex utility determines whether a discrepancy exists between the settings and the device that is attached. By reporting that no entries exist in the event log, the utility indicates that it does not detect any discrepancy.

Using the Bug Toolkit

If you have an account with Cisco.com (Cisco Connection Online), you can use the Bug Toolkit to find caveats for this product.

To use the Bug Toolkit, go to this URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have.PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems, Inc.
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html